NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXTENDING WI-FI DIRECT FOR AUTOMATED OPERATIONS

by

Aurelio Monarrez Jr.

March 2015

Thesis Advisor: Gurminder Singh
Co-Advisor: Raymond Buettner

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
EXTENDING WI-FI DIRECT FOR AUTOMATED OPERATIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Aurelio Monarrez Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

During a large-scale disaster, first responders face a number of different challenges. Their ability to communicate with each another is among the most critical challenges they face. If the disaster has wiped out the infrastructure that enables communications, it creates a serious issue for first responders. In such situations, infrastructure-less technology could enable first responders to establish a communications network independent of any existing operational or non-operational infrastructure. Wi-Fi Direct can enable such communication, but it is fraught with issues that need to be addressed to make it usable for first responders. An extension to Wi-Fi Direct has been developed that would address these issues. The extended Wi-Fi Direct protocol allows for a persistent communications network that involves zero user interaction. The extensions to the protocol do not require any infrastructure or any human involvement to establish a communications network.

14. SUBJECT TERMS Wi-Fi Direct, Wireless, Peer to Peer, Persistent Wireless	**15. NUMBER OF PAGES** 57
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EXTENDING WI-FI DIRECT FOR AUTOMATED OPERATIONS

Aurelio Monarrez Jr.
Civilian, Department of the Navy
B.S, Naval Postgraduate School, 2012

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2015

Author: Aurelio Monarrez Jr.

Approved by: Gurminder Singh
Thesis Advisor

Raymond Buettner
Co-Advisor

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

During a large-scale disaster, first responders face a number of different challenges. Their ability to communicate with each another is among the most critical challenges they face. If the disaster has wiped out the infrastructure that enables communications, it creates a serious issue for first responders. In such situations, infrastructure-less technology could enable first responders to establish a communications network independent of any existing operational or non-operational infrastructure. Wi-Fi Direct can enable such communication, but it is fraught with issues that need to be addressed to make it usable for first responders. An extension to Wi-Fi Direct has been developed that would address these issues. The extended Wi-Fi Direct protocol allows for a persistent communications network that involves zero user interaction. The extensions to the protocol do not require any infrastructure or any human involvement to establish a communications network.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AP	Access Point
API	Application Programing Interface
BSS	Basic Service Set
HA	Humanitarian Assistance
DFA	Deterministic Finite Automaton
DR	Disaster Relief
FA	Finite Automaton
FHS	Frequency Hoping Synchronization
GO	Group Owner
ISM	Industrial Scientific Medical
LAN	Local Area Network
MAC	Medium Access Control
OS	Operating System
NIC	Network Interface Card
P2P	Peer to Peer
TLV	Type Length Value

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my advisors, Dr. Gurminder Singh and Dr. Raymond Buettner, for their support and patience through this entire process. Their guidance and knowledge facilitated this research.

I also would like to thank Doug Horner, Robert Monarrez, Omar Monarrez, Lindsay, and Nick Golubev for their help.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In the last year, we witnessed an addition of 497 million mobile devices to the already existing 6.9 billion in 2013. Altogether, there are more than 7.4 billion mobile devices in use worldwide. In 2014, an addition of 439 million smartphones accounted for an 88 percent of the total growth in cellular phones [1]. The accessibility of mobile devices has revolutionized the way people use, access, and exchange information.

One method for exchanging information over these devices is through the use of Wi-Fi Direct [2]. Wi-Fi Direct is a relatively new wireless protocol. This protocol allows for Peer-to-Peer (P2P) mobile Ad Hoc networking. Wi-Fi Direct benefits from the strengths of the Wi-Fi standard—performance, security, and ease of use—and adds a number of new functionalities. These added functionalities include: automatic device discovery, a mutual awareness of capabilities between devices (inter-device capability awareness), sophisticated power management, and Infrastructure-less connectivity. Connections between these devices can happen anytime and anywhere. When devices come within range of one another, a connection request is sent. Upon request acceptance, a P2P Group is established and communication is enabled. To enable communication, one of the devices assumes the role of P2P Group Owner (Soft Access Point) while the others become P2P Clients. However, there is a drawback to this protocol.

A. PROBLEM AREA

While Wi-Fi Direct provides many useful features and functionality, a significant drawback of Wi-Fi Direct is that it does not allow the transfer of the Group Owner role. Upon device discovery, one of the devices assumes the role of Group Owner (Soft Access Point). This role cannot be transferred. Therefore, when the Group Owner leaves, the network collapses. There are two methods in which a Group Owner can leave the network. In the standard method, a user must manually press the disconnect button. Once the disconnect button is pressed, the Group Owner stops assuming the role of a software access point and connectivity between all devices stops. The other method in which the Group Owner leaves the network is a catastrophic failure or loss of power to the device.

In this case, the network gets destroyed and connectivity between all the devices stops. In either case, once the Group Owner leaves, a permanent interruption to the network occurs and all communication between devices ceases [3].

B. OBJECTIVE

An extension is proposed to extend the Wi-Fi Direct protocol to prevent the network from collapsing when the Group Owner has to change. This would allow for a more persistent network using Wi-Fi Direct.

There are many scenarios, such as Humanitarian Assistance and Disaster Relief (HA/DR) operations, disconnected military small unit operations, and other situations involving people disconnected from the Internet, where this extended protocol would have a significant and large impact [3].

C. METHODOLOGY

A detailed review of the Wi-Fi Direct protocol will be completed before developing schemes to extend the protocol. The focus will be on how group ownership gets established and how groups in general are formed. There will also be a comparison of other technologies that are used to exchange information wirelessly. A discussion illustrating the importance of new protocol using a HA/DR operation use case is provided as the basis for comparing alternate schemes. A suitable approach for transferring group ownership will be selected for implementation. The next step will be to implement the determined approach. Once implementation has been completed, lab testing will be conducted.

D. THESIS STRUCTURE

The structure of this thesis is as follows:

Chapter II provides the background for the work. This includes an overview of Wi-Fi 802.11, Wi-Fi Direct and Bluetooth. A comparison of these technologies is provided. A discussion of a use case for the extended Wi-Fi Direct protocol is also covered.

Chapter III covers the design and protocol extension. Several possible protocol extensions are considered. The recommended approach will be selected. This chapter also describes the design and model of the extended protocol.

Chapter IV describes the implementation and testing. Implementation is done using several mobile devices. All of the testing is conducted in a laboratory environment.

To conclude, Chapter V summarizes the work and provides recommendations for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

This chapter covers specifications of Wi-Fi, Wi-Fi Direct and Bluetooth. Also a comparison between each of these protocols is provided. In addition, a use case for the extended Wi-Fi direct is discussed. The emphasis is on the different types of wireless technologies and how each works.

A. WIRELESS TECHNOLOGY

Wireless technology has revolutionized how information is exchanged between people, and more specifically devices. Prior to the advent of the wireless technology, all information exchanges were made using physical, wired connections. Wireless technology has allowed for greater mobility, which has allowed for innovative solutions to everyday problems. We are now able to receive and exchange information freely in almost any place and at any time. Technologies that have enabled this exchange of information include Wi-Fi, Wi-Fi Direct and Bluetooth.

B. WI-FI

Wi-Fi—Wireless Fidelity—is based on the IEEE 802.11 standard. The most common use of Wi-Fi is for Internet connectivity in a local area network (LAN). A wireless LAN, which has a radius of tens of meters, consists of wireless devices that transmit and receive packets to and from a base station. A base station in Wi-Fi is also commonly known as an Access Point (AP).

1. Architecture

In Wi-Fi, a basic service set (BSS) is the fundamental building block of a wireless LAN. A BSS can have one or more wireless devices and a central base station. Just like any Ethernet device, a wireless device has a 6-byte MAC (Medium Access Control) address that is stored in the firmware of its NIC (Network Interface Card). So the APs wireless interface will also have a MAC Address. IEEE manages the distribution of MAC addresses, and each is globally unique. Wireless LANs require infrastructure and are sometimes referred to as infrastructure wireless LANs [4]. Figure 1 illustrates a basic wireless LAN.

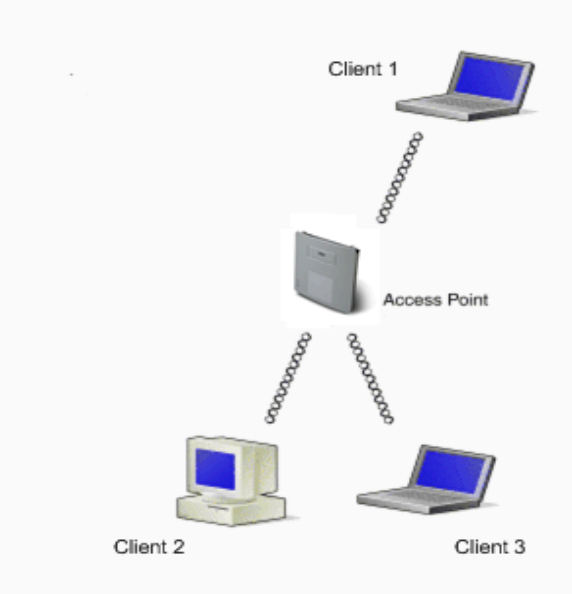

Figure 1. Illustrates a Basic Wireless LAN, from [5]

2. Access Point

In a wireless network, an AP is the key element of the infrastructure. The AP is responsible for sending and receiving data between clients. It also manages the coordination of multiple clients transmitting. Hotspots are used for Internet connectivity via mobile devices and cell service providers. An AP establishes communication by the use of scanning. An AP can perform two types of scans. The first type is when it scans for channels and listens for beacon frames. This type of scanning is referred to as passive scanning. The other type of scanning is known as active scanning. Active scanning is accomplished by broadcasting a probe frame to be received by any AP within its wireless range. In passive scanning, the first step is for a beacon frame to be sent out from the AP. Then the next step is for an association request to be sent from the client to the AP. In the final step, an association response is sent from the AP to the client. For active scanning, the initial step is a probe request frame that gets broadcasted to all AP. Then each AP will send a probe response. Followed by an association request frame sent from the client to every AP. To conclude, an association response is sent by all AP to the client [6].

3. Standards

There are multiple standards of 802.11, which currently include 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac. There are some devices that can operate in dual mode (for example, 802.11a and802.11g) or tri mode (for example, 802.11a, 802.11b and 802.11g). Table 1 illustrates each standards frequency range and data rate.

Standard	Frequency Range	Data Rate
802.11a	5.1-5.8 GHz	Up to 11Mbps
802.11b	2.4-2.485 GHz	Up to 54 Mbps
802.11g	2.4-2.485 GHz	Up to 54 Mbps
802.11n	2.412-2.484 GHz	Up to 300Mbps
802.11n	5.180 -5.809 GHz	Up to 300 Mbps

Table 1. Illustrates Each Standards Frequency and Data Rate, after [6]

C. WI-FI DIRECT

Wi-Fi Direct benefits from the strengths of the standard Wi-Fi, which include performance, security, and ease of use, and adds a number of new functionalities. These new functionalities include: automatic device discovery, a mutual awareness of capabilities between devices (inter-device capability awareness), sophisticated power management, and infrastructure requirement. Connections between these devices can happen anytime and anywhere, allowing for device-to-device communication. P2P devices support both Group owner (GO) and Client roles. These devices negotiate to establish Group Owner and client roles. Group Owners are essentially software APs. They can provide communication between clients and access to a concurrent WLAN connection.

1. Topology

The topology for Wi-Fi Direct can be one to many, such that several clients can be connected to one Group Owner The set of connected devices is known as a P2P group. Figure 2 shows a one-to-many relationship. The topology can also be one-to-one as depicted in Figure 3.

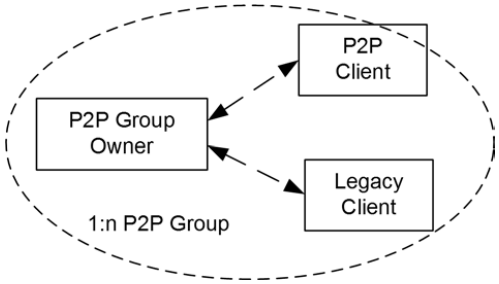

Figure 2 One-to-Many Relationship Group Owner Is Connected between Two Devices and Is Acting as the Software AP, from [3]

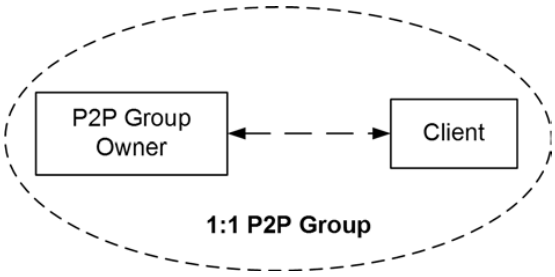

Figure 3. One-to-One Relationship, from [3]

A P2P device can operate simultaneously with a WLAN (see Figure 4). That device is known as a P2P concurrent device Any device performing concurrent operations requires multiple MAC entities. A concurrent operations device can operate on the same or different class and channel as a P2P group. For example, P2P may operate on channel 6 in the 2.4 GHz band, while the WLAN BSS can operate on channel 36 in the 5.8 GHz band. Concurrent operations are depicted in Figure 4.

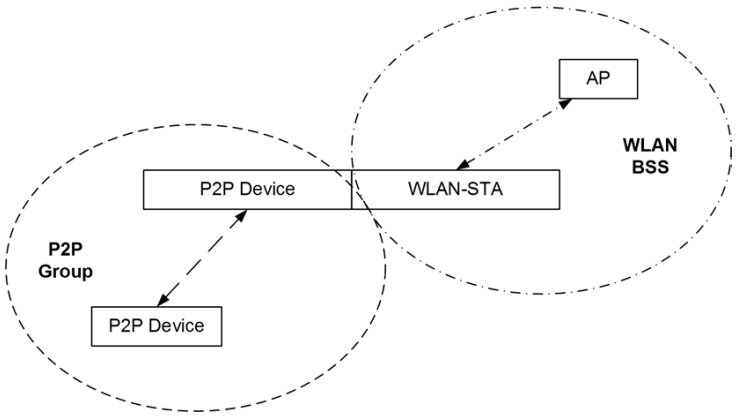

Figure 4. Simultaneous Connection to a P2P Device and a Wireless AP, from [3]

2. Device Discovery

Device discovery enables P2P devices arriving on the same channel to exchange device information. The purpose of the P2P device discovery is to rapidly determine which devices will attempt a connection. Device Discovery is made up of three major phases: Listen, Scan and Find.

In the listen phase, a device that is not in a P2P group can become discoverable. There are 3 predetermined listen channels. These channels, also known as social channels, are 1, 6 and 11 in the 2.4 GHz band.

P2P devices use the scan phase to locate the best operating channel for group formation and to find other P2P devices and Groups. By scanning all supported channels, devices in the scan phase collect information about surrounding devices and networks. A device can limit its scan to specific P2P devices or Groups. For devices, the limitation can be to specific device types.

The find phase is used to enable communication by ensuring that two P2P devices searching at the same time arrive to a common channel. This is accomplished by cycling between states. Randomizing the time spent on each cycle of the listen state enables convergence of two devices on the same channel. Limiting the list of channels to the

social channels minimizes the convergence time. Figure 5 illustrates the device discovery procedures.

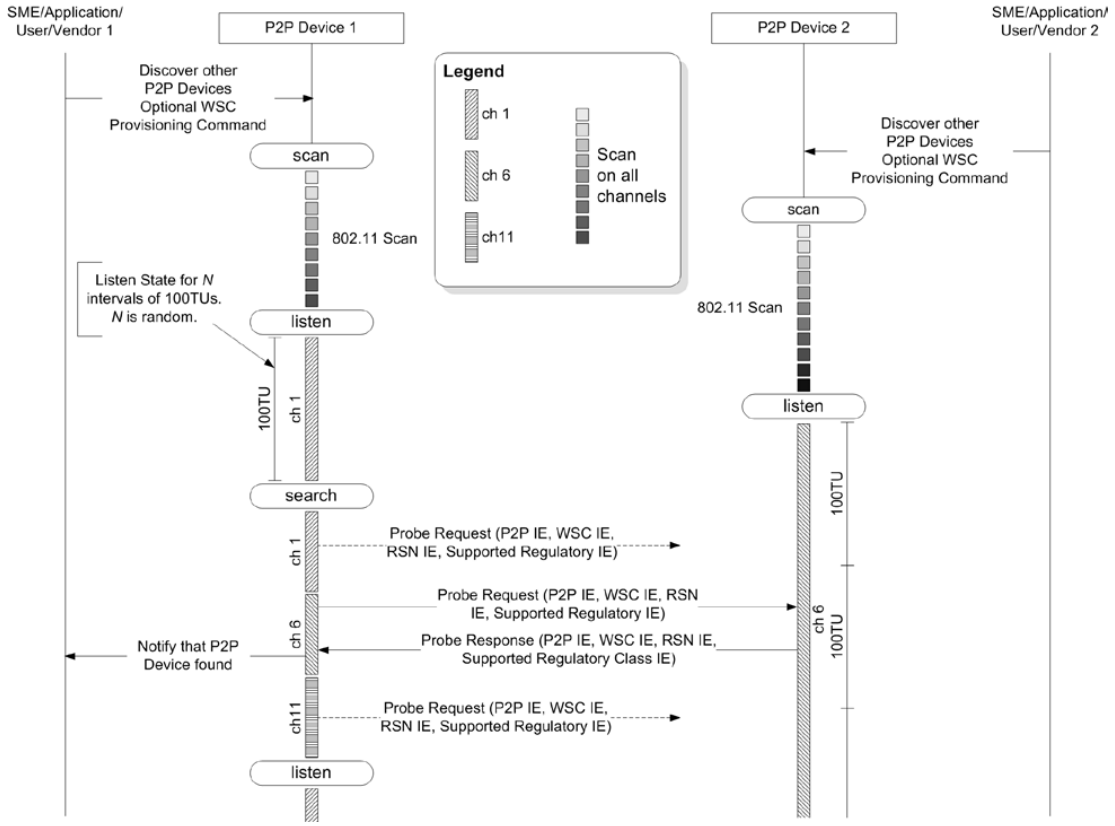

Figure 5. Device Discovery Procedures for a P2P Device, from [3]

3. Invitation Procedure

The invitation procedure is used in three cases: when a device receives an invitation by a Group Owner to become a client in the group, when a client invites another device to become part of their existing group, and when a Group Owner chooses to invoke a P2P Persistent Group.

a. Invitation Request

A Group Owner or a client can send out an Invitation Request. When the Group Owner sends out an invitation request, it contains the Group ID, Group BSSID, Channel

List, Operating Channel and Configuration Timeout Attributes. A request that is sent by a client will contain the Group ID, Group BSSID and Configuration Timeout Attributes.

b. Invitation Response

A device that receives an Invitation Request will respond by sending an Invitation Response. A Response sent by a Group Owner will contain, Group BSSID, Channel List, Potential Operating Channels, Indented Operating Channel, Configuration Timeout Attributes and the Group Owner Configuration Time. An invited client will respond by sending a response that contains the Channel List and Configuration Timeout Attributes. All supported Operating Channels will be indicated on the Channel List. Only Channels indicated on the Channel List from the Invitation Request will be on the Invitation Response Channel List. Configuration time will be indicated in the Configuration Timeout attribute, which will include the point that the client is ready to join the group until after the Invitation Response indicates a success.

c. Group Owner Negotiation

The Group Owner Negotiation happens through a three-way handshake. When a device comes within range of another device, it sends a Group Owner negotiation request. In the request there is a Group Owner intent field. In this field the device can set a value of 0 to 15. Devices that require Group Ownership in order to work properly will set a value of 15. Those devices that do not require being a Group Owner will have a lesser value. The second device will then send a Group Owner negotiation response with its own Group Owner intent. If there is a tie between the two devices, the Group Owner will be determined by the tiebreaker bit. The tiebreaker bit gets set randomly when each device gets powered on. The bit consist of 1 or a 0, the device that has a value of 1 will become the Group Owner. The network gets established when the first device sends a Group Owner negotiation confirmation. One device becomes the Group Owner while the others become P2P Clients. Figure 6 illustrates the Group Owner Negotiation. Group Owner determination is illustrated in Figure 7.

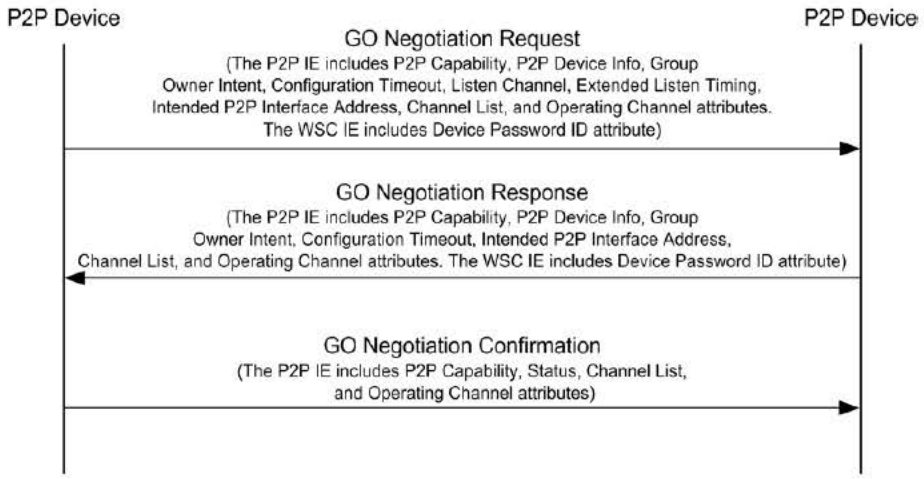

Figure 6. Group Owner Negotiation, from [3]

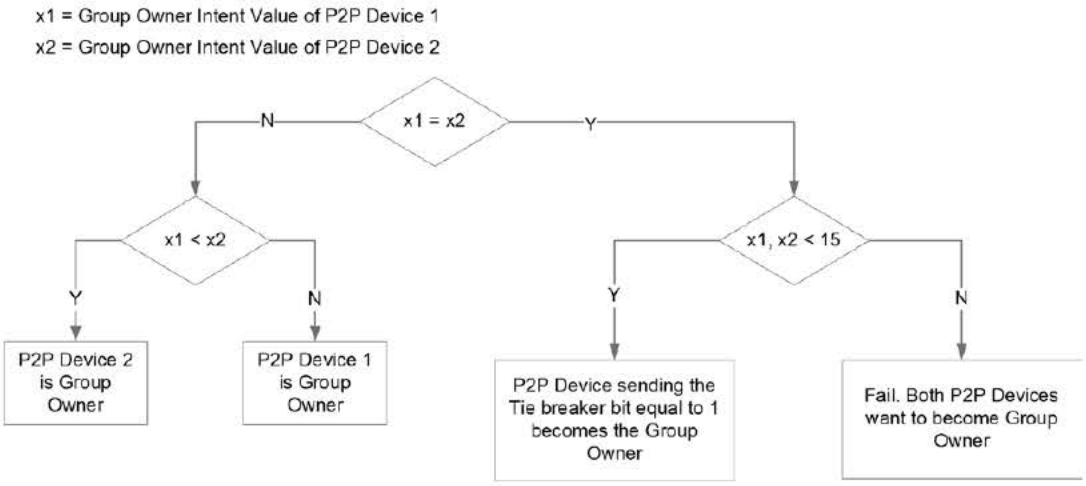

Figure 7. Group Owner Intent Negotiation, from [3]

4. Invoking a P2P Persistent Group

Once a device successfully obtains credentials from a group, it stores the P2P Group ID and Credentials for that group. This allows the Group Owner to recreate a session at any time after the initial formation. Clients can also use the stored credentials to request a Persistent Group be started. The Group Owner has the option of maintaining a list of device addresses that have joined the Persistent group. For each session, the

Group ID and Credentials will not change, although the interface address and operating channel can change for each session [3].

D. WI-FI HOTSPOTS

A Wi-Fi Hotspot or tethering is a method for accessing the Internet via a mobile phone. This method enables a mobile phone to use its cellular connection to provide access to the Internet. A mobile device can connect to a mobile phone through Wi-Fi. Almost all devices in the United States can support up to 5 devices being tethered to one mobile phone. While at the surface level there may seem a lot of similarities between Wi-Fi Direct and Wi-Fi Hotspots, the two technologies are quite different. Wi-Fi Hotspots require physical infrastructure to work. The infrastructure is the cellular infrastructure that provides access to the Internet. In addition, the AP functionality supported by the Wi-Fi Hotspot phone does not go through the process of Group Owner negotiations as the device that creates the AP is the equivalent of a Group Owner. Wi-Fi Hotspot set-up also does not support the advanced power management features supported by Wi-Fi Direct.

E. BLUETOOTH

Bluetooth is another technology that allows devices to communicate wirelessly in ad-hoc networking modes. The main features of Bluetooth consist of it being low power and low cost. Almost all mobile devices in the U.S. are equipped with Bluetooth. Paring is when two Bluetooth enabled devices connect to each other. In order for these devices to pair, they need to be in proximity of one another. Establishing a connection allows the two devices to share information wirelessly. These networks are established automatically and dynamically as devices come within range of one another. Bluetooth has the ability to transmit voice and data simultaneously. Bluetooth operates in the 2.4 to 2.48GHz unlicensed industrial, scientific and medical (ISM) band. There are 3 Classes of Bluetooth radios, Class 3, Class 2 and Class 1. Class 2 radios are found in mobile devices. They have a range of about 10 meters or 33 feet [7].

1. Connectivity

A Bluetooth network is known as a piconet. A piconet is a set of at most seven devices; a single device controls each piconet. The six other non-controlling devices can be connected to other piconets simultaneous as well. A group of piconets is known as a scatternet (Figure 8). The piconets do not need to be interconnected in the scatternet, but can be. The controlling device is called a master. The device that accepts the request becomes the slave. The master controls the channel and all the slaves operating on that channel. All Bluetooth devices are identical except for a unique 48-bit device identifier [8]. The symbol m indicates a device is a master, and the symbol s indicates a device is a slave.

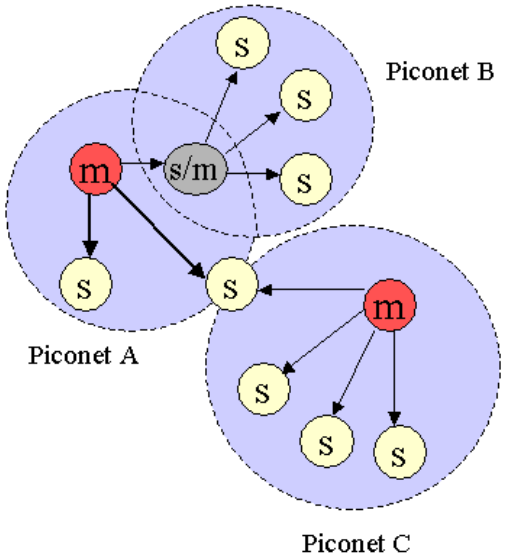

Figure 8. Piconets Making up a Scatternet, from [9]

2. States

The two main states for Bluetooth are Standby and Connection. There are seven other interim states that are used to add new slave devices to a piconet. The seven other states are Inquiry, Inquiry Scan, Inquiry Response, Page Scan, Page, Slave Response and Master Response.

a. Standby

When a device initially powers up Bluetooth, it will be in the default state, which is called the standby state. If this same device sends a connection request and it receives a reply from another device, then it will immediately transition into the connection state as a master. Otherwise, if the device receives a connection request and replies with an acknowledgement, it will immediately enter the connection state as a slave.

b. Inquiry, Inquiry Scan, Inquiry Response

The purpose for the Inquiry set of states is to allow a device to determine which devices are available within transmit and receive range. A device uses Inquiry Scan to scan on a frequency. In the Inquiry state, a device can query another device that is in the Inquiry Scan state. A Connection state cannot be reached from an Inquiry state. The purpose of Inquiry Respond state is to transition out of the Inquiry Scan state. This is accomplished by a device in the Inquiry scan state, responding to a request from a device in the Inquiry state.

c. Page Scan State

The Page Scan state can be entered from the Standby or Connection states and scans a single hop frequency, 11.25ms. In order for a device to enter the Page Scan State from a Connection State, it must free up as much available scan time as possible. The Bluetooth device's address determines the scan frequency.

d. Page State

When a device establishes a connection with a slave device, this state is known as the Page State. In this case, the master device determines what frequency to transmit the page on.

e. Slave Response/Master Response State

An initial Packet ID is sent from the Master to the slave. Then the Slave will respond with its own Packet ID. Followed by the Master sending a Frequency Hoping Synchronization (FHS) and the Slave responding with an acknowledgment of the Packet

ID. To conclude, after a successful exchange of information both devices can start communicating with each other.

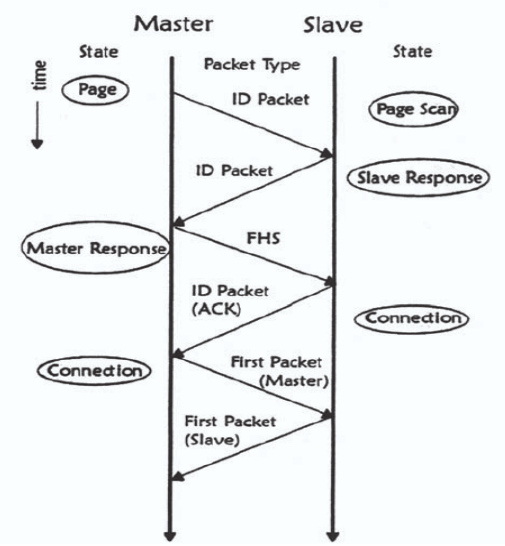

Figure 9. The Process by Which Messages and States Progress as a Page Request Is Serviced, from [8]

f. Connection State

This is the state where the master and slave devices exchange information. In order for the master device to determine if the slave device is using the correct frequency-hopping scheme, and that the clocks are synchronized, the master will send the slave a POLL request. If the slave does not receive the POLL request or if the master does not receive a response then both devices will return to the Page/Page Scan state. The Connection state is terminated through a "reset" or "detach" command. The link parameters are maintained when a termination is executed through the "detach" command. When the reset command is executed, all existing configuration information gets eliminated.

3. Service Discovery

Service Discovery is an optional frame exchange that can be done with any discovered devices. This exchange is done prior to any group formation and is done for

the purposes of verifying compatibility of services offered between each device. This service is adaptable and extendable to allow higher layer service protocols such as Plug and Play. The Service Discovery is used to find the following: all services offered by a device, information about a specific service offered by a device, information about various services offered by a device, and if a change has occurred in the services that a device offers. A Service Discovery Query initiates Service Discovery.

F. COMPARISON

Each of the wireless technologies described above have many attributes that are common while others are different. While each has its advantages and disadvantages, a particular technology can clearly serve as an optimal solution for several a select set of use cases.

1. Wi-Fi versus Wi-Fi Direct

Wi-Fi and Wi-Fi Direct are very similar when it comes to functionalities and capabilities. However, there are some major differences. Both of these protocols allow for the wireless exchange of information between devices. While Wi-Fi has been around since the 1990s, Wi-Fi Direct has come into existence since 2010.

a. Similarities

Both technologies can operate in the same ISM frequency band of 2.4 GHz. They also have the same range and data throughput. Furthermore, they use a base station-client model where one device acts as a base station and the other devices are clients.

b. Differences

Wi-Fi is completely dependent on infrastructure, meaning that an AP (hardware) is required in order for this protocol to work. Wi-Fi Direct, on the other hand, requires no infrastructure allowing for mobile ad-hoc networks to be created anywhere and anytime. It utilizes a software AP, meaning any device can act as an AP. Not depending on infrastructure increases the mobility of Wi-Fi Direct. Devices utilizing Wi-Fi Direct can also simultaneously use Wi-Fi. This would be extremely useful in environments where

you have limited infrastructure. In addition, Wi-Fi Direct has a power management feature that is used to conserve battery power on all devices including clients and APs. This feature is very useful in environments where the ability to charge mobile devices might be limited. While both technologies can operate in the same 2.4GHz ISM band, Wi-Fi has the ability to operate in the 5.8GHz band as well.

2. Wi-Fi Direct versus Bluetooth

Both technologies are very similar with some differences. They both allow for the wireless exchange of information. Also, both of them can be used for mobile ad-hoc networks.

a. Similarities

Bluetooth and Wi-Fi Direct do not require any infrastructure in order to work. This allows for either to set up a mobile ad-hoc network anytime and anywhere. Both of these technologies require one device to act as a Group Owner or Master device, while the other devices in the network become Clients or Slaves. Furthermore, they both operate in the ISM band.

b. Differences

Bluetooth is limited to seven devices being connected in a piconet (Bluetooth network). Wi-Fi Direct does not have the same limitation. Bluetooth is also limited to a range of 10 meters (33 feet) whereas Wi-Fi Direct has a range of about 100 meters. Bluetooth limitations can prove to be very constraining in certain environments, specifically, where you require more than 7 devices and a range greater than 10 meters.

G. EXTENDED WI-FI DIRECT USE CASE

An impactful use case would be the use of this protocol by first responders in a HA/DR environment. Currently communication between mobile devices relies on local and physical infrastructure. First responders cannot rely on the availability of infrastructure while in disaster areas, or even on that infrastructure to work. That said, first responders equipped with mobile devices that include the extended Wi-Fi Direct

could rapidly establish a mobile ad-hoc communications network. This network would allow information exchange between government, NGO's and civilian responders.

1. Hurricane Katrina

In 2005 Hurricane Katrina had a devastating impact on the Gulf Coast. It is estimated when Katrina made landfall, it was a Category 3 Hurricane (Winds of 111–113 MPH) with sustained winds of 125 MPH. The force of these winds, along with storm surges and flooding, damaged or destroyed the communications infrastructure.

Communications infrastructure was one of the most affected critical sectors by Hurricane Katrina. Commercial power failed and forced 180 central office locations to run on generators. An estimated 100 commercial radio station towers were taken off the air. Land Mobile radio was greatly degraded, and as many as 2000 cell towers were taken out. Most of the backbone conduit that supported landline services was flooded. Not all communications were taken out by the storm though. For example, satellite phones could be used once the storm passed, but there were very few to go around. Eventually, the satellite phones ran out of battery power [10].

2. Hurricane Sandy

In 2005 Hurricane Sandy made landfall in the northeastern part of the United States. It was a category I hurricane with sustained winds of 80 to 90 MPH. Although this hurricane was not as severe as Katrina, it still had a significant impact on the communications infrastructure.

It was estimated that about 25 percent of cellular base stations in the affected area lost service. Most base stations' loss of service was due to lack of power. Direct damage, flooding and power outages directly affected wireline telephony outside plant equipment. Internet has become a vital need during disasters. During Hurricane Sandy several data centers experienced issues and loss of service [11].

3. Summary of Use Cases

A persistent network that requires no infrastructure would facilitate sharing of information in a disaster area. Wi-Fi Direct increases mobility and portability by allowing devices to connect anywhere and anytime. Extending Wi-Fi Direct will establish a persistent network for sharing information.

III. EXTENDED WI-FI DIRECT DESIGN AND MODEL

In this chapter we will cover the two proposed solutions for the extended Wi-Fi Direct design. The best solution will be chosen and a model of it will be given. The model will be represented using a Deterministic Finite Automaton.

A. PROTOCOL EXTENSION

A consideration of two methods for extending the Wi-Fi Direct protocol will be performed. The two methods will recommend different approaches for extending the standard Wi-Fi Direct protocol. More specifically preventing a permanent network disruption when an existing Group Owner leaves the group. The first is to simply make a back up of the Group Owner. Once a back up is made, a transition of group ownership will occur when the existing Group Owner leaves. The other is to make a persistent protocol by fully automating Wi-Fi Direct. This will automate everything from establishing Wi-Fi Direct groups to the migration of Group Owners.

1. Back Up Group Owner Approach

The first solution involves making a back up of the key attributes and configuration of the Group Owner. When the Group owner is no longer present, the designated device would take its place. In this approach, we decided that the first device that connected to the Group Owner would assume the role of back up. When the Group Owner leaves, the designated device assumes the role of the new Group Owner. There were many details that had to be kept track of in order for this solution to work. Among many of the details, the most important were: the Group Owner's IP address, device name, and mac address The Group Owner IP is not given in the standard protocol. In order for us to find the IP address, we had to create a method that would give it to us. The device name and mac address are given in the standard protocol and those were simply copied. Checking for a constant can monitor the Group Owner's connectivity. This constant informs the devices in the network whether they are connected to the Group Owner. The difficulty with this solution is forcing a device to be a copy of the Group Owner. The back up device would have to have the same IP, device name, and mac

address in order for this solution to work. Another issue is what happens when the old Group Owner tries to re-join the network. This causes an IP conflict because there are two devices with the same IP. Not to mention, you wouldn't be able to ensure proper routing with two identical devices. The biggest issue is a device can only monitor when a Group Owner is disconnected. Which means, a device only knows when the network has collapsed completely. Once the network has collapsed, re-establishing of the network must be done with the back up Group Owner. Rather than keeping track of all the details; a more streamline approach was developed. Figure 10 illustrates what the initial stage in the back up Group Owner model would look like. Figure 11 shows what would happen after the Group Owner has left and the back up has replaced it.

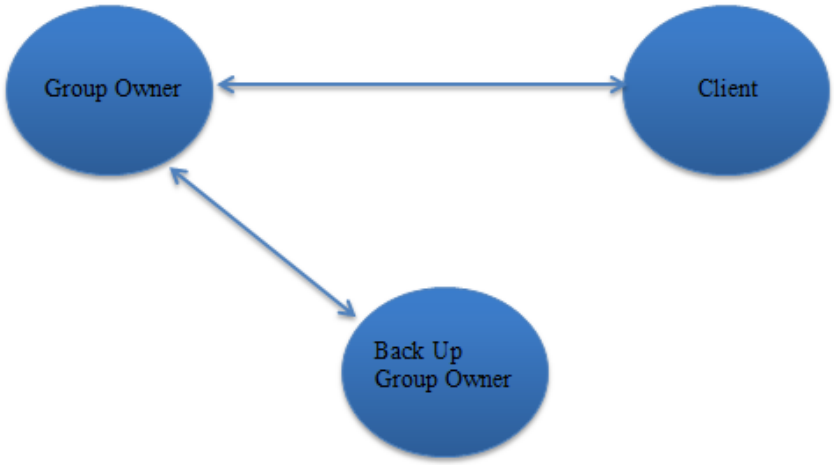

Figure 10. The First Iteration of the Back Up Solution

Figure 11. The Second Iteration of the Back Up Solution

2. Automated Persistent Approach

The other potential approach was to automate the protocol. Automation would provide ease of use and a seamless Group Owner migration. From establishing Wi-Fi Direct groups to the migration of Group Owners, we automate each step in the entire process. The first step is to automate the peer discovery. In the normal protocol this is done manually by selecting a button on the user interface. In our extension, any device using Wi-Fi direct would automatically perform the peer discovery on start up. We pre-provision all devices that are allowed to form a network with the MAC addresses of the entire group. This enables us to ensure that unauthorized devices do not join the network.

The next step is to automate the group formation request. Normally, a user has to manually select a peer from the device's peer list and manually send the request. We have automated this by sending the request to the first peer on the device's peer list. The subsequent step is to automatically accept the group request. In the normal protocol, a user would have to manually click on a button and accept the request. In the extended protocol the group acceptance is done automatically without user interaction.

In our extension of the protocol, the first peer on the peer list is selected to be next Group Owner. This does not have to be the case, Criteria such as battery status, shared responsibility in a round robin fashion, special designation, or location can also be used to determine Group Owner selection automatically.

In our extended protocol, we monitor for the disconnection in the network through Group Owner departure. Once we know that the Group Owner has left, we clear each device's peer list, automatically perform a peer discovery, and begin the connection process over. Figure 12 shows the normal timing diagram for establishing a network. Figure 13 shows the timing diagram for the extended Wi-Fi Direct protocol.

3. Differences Between the two Approaches

There are several differences between the two approaches discussed above. In the back up approach, each device in the network needs to maintain the entire detail about the network. Having to implement this approach can be problematic because of its complexity. Access to the Operating System (OS) would be required to get access to each

device IP. The Google API does not allow access to the OS. The automated approach is the simplest method to implement and can be done by using the Google API Wi-Fi P2P.

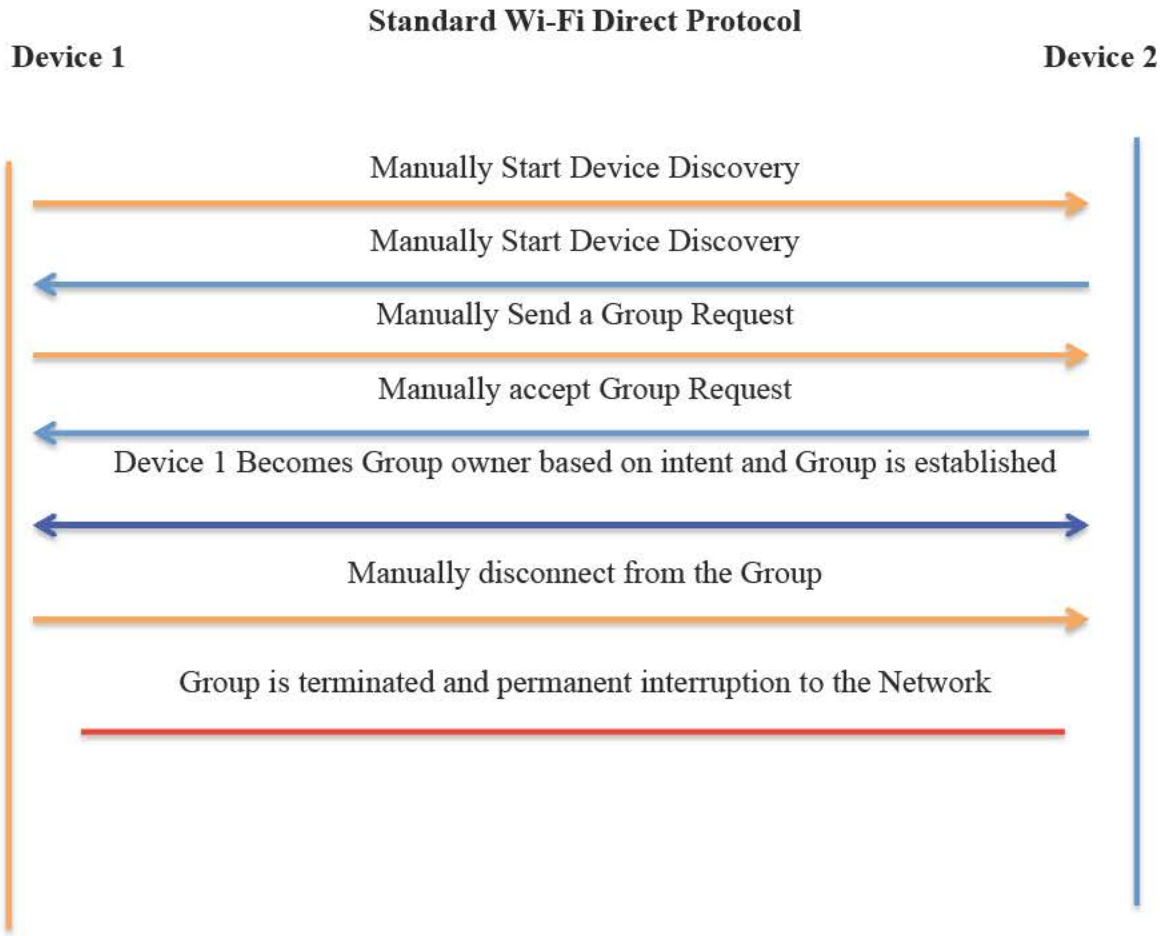

Figure 12. The Normal Sequence for Group Formation. It also Shows the Permanent Disruption to the Network, from [3]

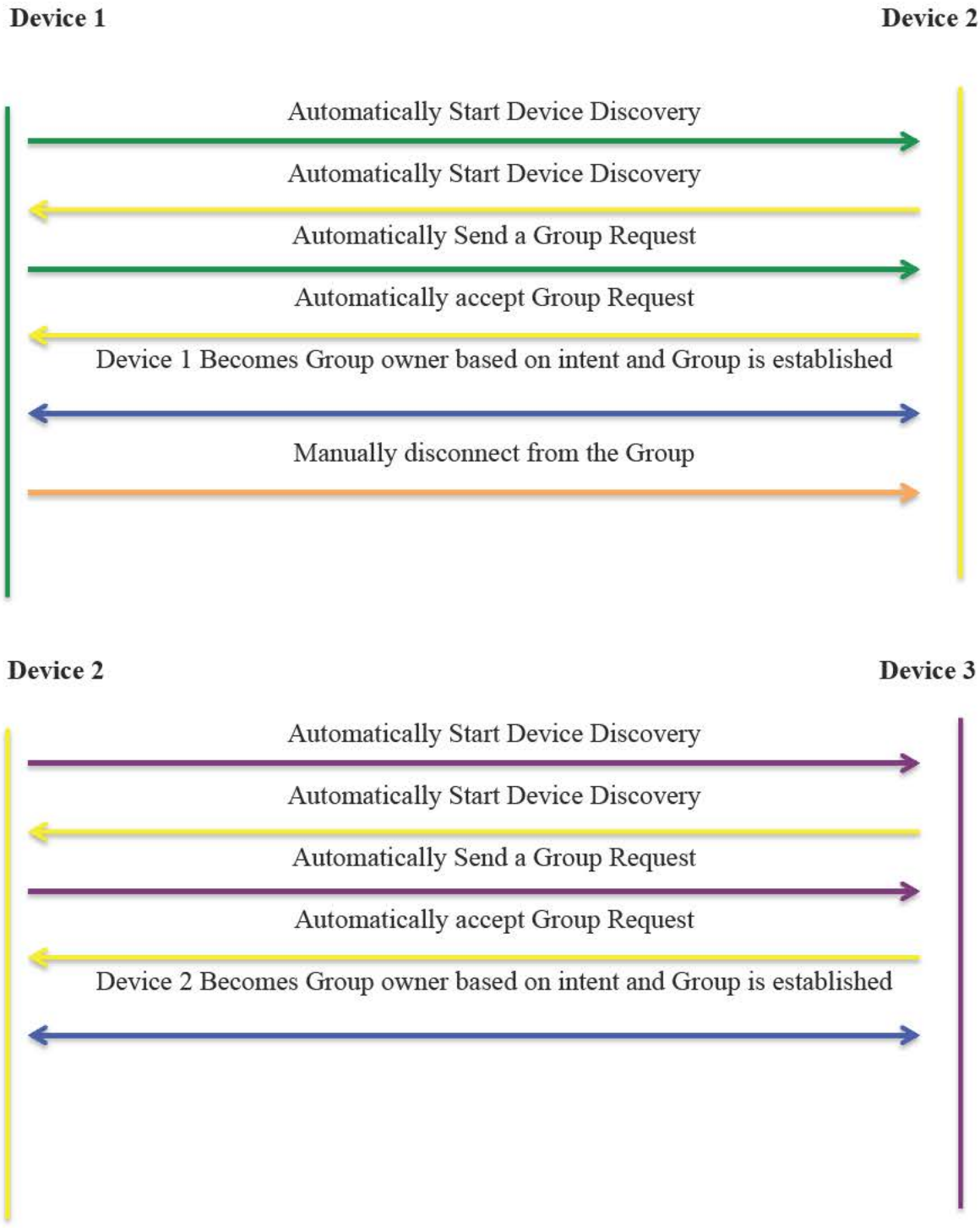

Figure 13. Shows the Extended Wi-Fi Direct

B. PERSISTENT SOLUTION MODEL

An automaton is a mathematical model of a computer that is used in string recognition. A finite automaton (FA) is an abstract machine used for string recognition. FA is defined as a 5-tuple (A, S, s_0, S_{acc}, R): A is the finite input alphabet, S are the finite set of states, s_0 is the start state where $s_0 \in S$, S_{acc} the set of accepting states where $S_{acc} \subseteq S$, and R is the state transition function where R: $S \times A \rightarrow S$. A Deterministic Finite Automaton (DFA) will be used to model the extended Wi-Fi Direct protocol. The state transition function does not allow more than one transition from any state for a given input alphabet symbol. The DFA will accept a string s, if there exist a path from a start state to an accepting state with transitions labeled with symbol of s [12].

1. DFA

The input alphabet or A is 0 and 1. The set of states or S, are s_0 and s_1. The start state is s_0. The accepting state or S_{acc} is s_1.

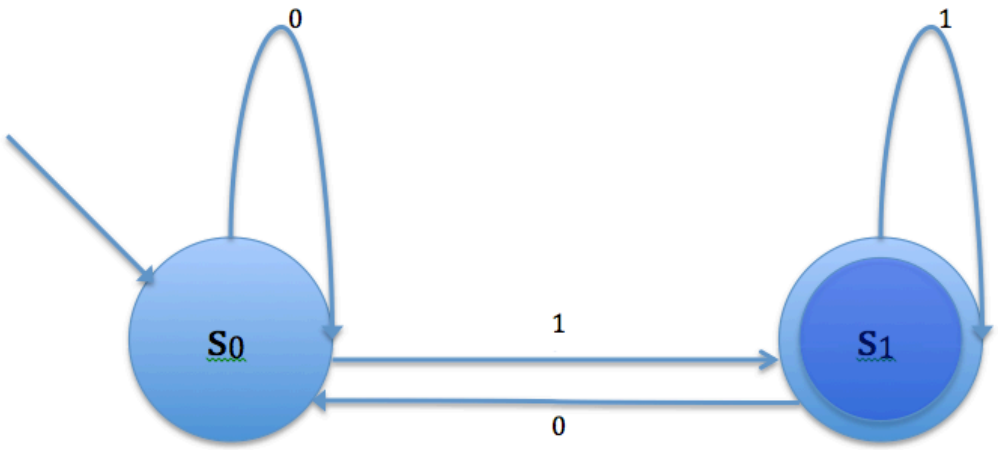

Figure 14. Illustrates the State Transition Function.

a. DFA Definition

State s_0 is defined as a state where the device is not in a group (disconnected). An input of 0 at state s_0 will cause the device to loop and continue to stay at state s_0. An input of 1 at state s_0 will cause a transition to state s_1. State s_1 is an accepting state, meaning the device has joined a group (connected). If at any point state s_1 receives an input of 0, it will immediately transition back to state s_0 where it will continue to try and get back to s_1. The device would stay or transition to state s_0 anytime it was not connected to any other device.

C. SUMMARY

In this chapter the two proposed approaches were discussed. They were then compared to each other. Furthermore, the automated approach was selected and a model was given. The model representation was of a DFA state machine. To conclude a definition of that DFA was given.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. IMPLEMENTATION AND TESTING

In this chapter we will cover the implementation and testing of the extended Wi-Fi Direct protocol. The Implementation was done using Google's API. We used Google's Wi-Direct Demo application for the initial set up of the standard Wi-Fi Direct protocol. The testing was conducted using Samsung S3 phones.

A. AUTOMATION

The first step was to automate the entire process for establishing the Wi-Fi Direct network. This meant automating the device discovery, group request, group acceptance, establishing and re-establishing of the network. The automation would allow for ease of use, and establishing and re-establishing of the network without any user interaction.

1. Device Discovery

In the normal Wi-Fi Direct protocol, the device discovery is done manually; the user has to manually push a button to initiate the peer discovery. For our extended protocol, we modified the WifiDirectActivity class. Here we implemented a discover loop in order to automatically perform peer discovery.

2. Auto Group Request and Accept

In the standard Wi-Fi Direct protocol, the group request and accept are done manually. The user has to manually select the device they want to send the request to by pushing a button. Once the request has been sent, the device that receives the request has to manually accept the request by pushing a button. In order for us to automate this process, we had to create our own AutoConnect class. This allowed us to automatically send and accept requests.

3. Establishing and Re-establishing a Group (Network)

In the standard implementation of Wi-Fi Direct, a group is established manually. Users must manually perform a peer discovery on each device, followed by one user sending an initial request. Then that request must be manually accepted, and

subsequently, all other devices can join by sending the Group Owner a request to join. The subsequent devices visually identify the Group Owner by looking at the device, ensuring they are sending the request to the right Group Owner. Re- establishing of the group is done manually by repeating the same, entire process. By Modifying the DeviceListFragment, WifiDirectActivity and Auto Connect classes, we have automated the establishing and re-establishing of the network [13].

B. IMPLEMENTING THE DFA MODEL

With automation completed, the next step was to implement the DFA model from Figure 16. The starting state for a device will always be at state s_0. Also, a device will be in state s_0 anytime it is not connected to a Group Owner. Using a constant flag that is set when a device is not connected allowed us to know when a device was in state s_0. As long as that constant was not present, the device would remain in state s_0. Once state s_0 received an input of 1 (constant was present), the device would transition to state s_1. The device would remain in the accepting state s_1 until it received an input of 0 (constant was no longer present). This implementation allowed for continual monitoring of the network. This allowed us to know when there was an interruption in the network and re-established the network when needed.

C. TESTING

During the testing there were significant hurdles that had to be overcome. There were difficulties with the initial peer discovery to establishing and re-establishing of the group. After exhaustive testing and troubleshooting, many of the hurdles were overcome.

1. Testing Configuration

Testing was performed using Samsung Galaxy S3 phones and a Mac Book Pro. Prior to any testing being done, the Mac Book Pro was configured with the Android Development Tool. To begin, each device was loaded with the Wi-Fi Direct demo application. Once the standard functionality of the demo code was checked, modifications were then done to the standard source code. The majority of modifications were done to the classes that support: Peer Discovery, Group Formation, and

Disconnecting. Subsequently before each test, the devices where loaded with the modified Google API Wi-Fi direct application. Each test ran from 10 seconds to 10 min in length. Initially each test was only conducted using two devices. As each test became more successful, the number of devices was increased.

Device	Operating System	Firmware	Processor	Memory
Mac Book Pro	OS X Yosemite	10.10.2	2.8GHz Intel i7	16 GB
Galaxy S3	Android	4.3	1.5 GHz dual core Krait	32 GB
Galaxy S3	Android	4.1.2	1.5 GHz dual core Krait	32 GB
Galaxy S3	Android	4.1.2	1.5 GHz dual core Krait	32 GB
Galaxy S3	Android	4.1.1	1.5 GHz dual core Krait	32 GB
Galaxy S3	Android	4.1.1	1.5 GHz dual core Krait	32 GB

Table 2. Details about the Devices Used for Testing

2. Discovery Loop

The initial bug found during testing was in the discover loop. During the coding there was no delay added to the discovery loop to allow for ample time to connect. This was causing the devices to continuously run the discovery loop causing an infinite loop; this did not allow enough time for the devices to connect to each other, resulting in neither device ever connecting. Upon further testing a time delay was added. The initial delay was 20 seconds. This allowed enough time to connect, determining the shortest time needed was the following test. Decreasing the time delay from 20 seconds to 1

second an ideal time was found. The ideal delay was determined to be 10 seconds, this allowed both devices enough time without excessive waiting.

3. Connecting

During additional testing, the devices would connect instantly and other times would take up to 10 minutes. During our troubleshooting, it was observed that this characteristic was not present in the original protocol. In the standard protocol, once a manual request and accept messages were exchanged, the group formation was almost immediate. The differences in the code from the original and extended protocol were the automation piece for the extended protocol. After extensive testing and searching it was concluded that the problem was with the automation code: after both devices automatically performed a device discovery, each would simultaneously send a request messages. In essence, both devices were trying to connect at the same time and therefore neither would end up connecting. The recommendation was to implement a random Boolean. This allowed only one device to send a request message while the other sent an acceptance. The issue was not present in the original protocol because the request and acceptance were done manually.

4. Re-establishing the Group

Another issue that had to be overcome was re-establishing of the network; the amount of time it took was significant compared to the initial set up. In the extended protocol, before re-establishing can occur, each device clears its peer list. This implementation was added because some devices would try to connect to a Group Owner that was no longer present. After being unable to connect, each device would eventually connect to a device that was present. This issue persisted on some devices. The issue was determined to be the firmware on the devices. Each device with Android firmware 4.2 or lower was unable to clear its peer list. This caused a grater delay in re-establishing the network.

5. Group Owner Identification

An additional issue discovered during testing was when a group was already established; a device trying to connect to the group could not connect. During the automation, when two devices discover each other, they connect to the first peer on the peer list. This was successful as long as there were only two devices present. The issue was when a third device tried to perform a peer discovery and the first peer on its list was not the Group Owner; it would try to connect to the group via a non-Group Owner. This would cause the device to continually try to connect unsuccessfully. In order to address this issue, a Group Owner check was implemented. Before a device attempted to connect to the first peer on its list, it now checks for a Group Owner. In effect, it determines if there is a group that has already been formed. If there is a Group Owner, the device would connect to the identified Group Owner, otherwise the device connects to the first peer on its list.

6. Dialog Box

A minor issue was after a group has successfully established; a dialog box would remain on each device indicating an attempt to connect. This issue was only present in the extended Wi-Fi Direct protocol. A modification to the DeviceListFragment class was made which forced the dialog box to close once a device successfully connected.

D. SUMMARY

This chapter provides the details of the initial implementation involved in the automation of the protocol. The major components that were automated were device discovery, group request and accept and establishing and re-establishing of the group. During the testing significant issues were encountered. After extensive testing and troubleshooting all of the issues were overcome.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

The purpose of this research was to extend the standard Wi-Fi Direct protocol. An initial review of this technology found several issues in the protocol that make it difficult to use in practice. The most significant issue was the permanent interruption to the network once a Group Owner leaves the network. A proposal of two approaches was given to address this issue. After careful analysis, we determined that the automated and persistent protocol would be the best approach for our needs. This approach further extends the standard Wi-Fi Direct protocol.

The extended Wi-Fi Direct protocol allows for more robust mobile ad-hoc P2P network in a HA/DR or military operations. The extended protocol's ability to prevent a permanent interruption to the network has made Wi-Fi Direct persistent. In an HA/DR environment a network interruption prevents communications between first responders. With the extended Wi-Fi Direct protocol, first responders can now keep constant communications in a HA or DR area. Also, the automation of the network formation eliminates the need for the user to establish a network manually. This augments any user with out having to burden them with knowing when and how to establish the network. The ideal use case for the extended protocol would be in an infrastructure less or limited infrastructure environment.

Future work can explore the development of the extended protocol, which has adapted Wi-Fi Direct into a persistent protocol. Additional research could be done to further develop the Group Owner back up model discussed previously. The biggest hurdle to overcome would be the re-establishing of the network. Once the network has been interrupted, the back up model is no longer viable. A seamless transition must occur in order for the back up model to be successful.

Transitioning the Group Owner role without any interruption is necessary for this model to work. This might require a completely new protocol to be developed. However, it is possible to modifying the existing Wi-Fi Direct protocol. Making a seamless transition would require a table to keep track of all the devices in the group. The table

would have information about each devices IP, device name and Mac Address. Also each device's Group Owner intent would need to be hard coded. The table would then combine the device specific information with the Group Owner intent to establish a back up order. Each device would have this information and would maintain it. One other requirement for this protocol would be a ping or heart beat to the Group Owner. This would monitor the presence of the Group Owner. If the ping or heart beat stops, then each device would know and the back up that is first on the table would take over.

Device	IP	Device Name	Mac Address	GO Intent
1	192.168.113.1	Phone 1	3E123A	15
2	192.168.113.2	Phone 2	3D123B	10
3	192.168.113.3	Phone 3	3F123A	5

Table 3. Example of What Each Device Would Have in the Back Up Group Owner 2.0 Model

In the example table above the initial Group Owner is phone 1. When that device leaves the group, it simply gets removed and phone 2 is moved up and assumes the Group Owner role. The table gets updated as new devices join and leave the group.

LIST OF REFERENCES

[1] Cisco. (2015). “Cisco visual networking index: Global mobile data traffic forecast update 2014–2019 white paper.” [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html. [Accessed: 12- Jan- 2013].

[2] Wi-Fi Alliance Technical Committee P2P Task Group. Wi-Fi Peer-to-Peer (P2P) technical specification, 2011. Version 1.2

[3] K. Robinson. Wi-Fi Peer-to-Peer Best Practices Guide, 2010. Version 1.0.0. Wi-Fi Alliance, December 2010.

[4] J. Kurose and K. Ross, *Computer Networking*. Boston: Pearson/Addison Wesley, 2008.

[5] Cisco. (2015). “Basic wireless LAN connection configuration example.” [Online]. Available: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/68005-wlan-connect.html. [Accessed: 20 Apr 2014].

[6] Cisco. (2015). “Cisco Connected Mobile Experiences (CMX) CVD – radio frequency operating and data rates [design zone for mobility].” [Online]. Available: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise /Borderless_Networks/Unified_Access/CMX/CMX_RFOpFreqDataRates.html. [Accessed: 04 Jan. 2014].

[7] Bluetooth.com. (2015). Basics. [Online]. Available: http://www.bluetooth.com/Pages/Basics.aspx. [Accessed: 06 Apr. 2014].

[8] W. Tranter. *Wireless personal communications*. Boston: Kluwer Academic, 2001.

[9] Oracle. (2015). Wireless application programming with J2ME and Bluetooth. [Online]. Available: http://www.oracle.com/technetwork/systems /index-156651.html. [Accessed: 07 Apr. 2014].

[10] Miller, Robert. *Hurricane Katrina: Communications & Infrastructure Impacts*. National Defense University, Fort McNair, Washington, DC, 2006.

[11] Users.ece.utexas.edu. (2015). [Online]. Available: http://users.ece.utexas.edu/~kwasinski/1569715143 Kwasinski paper FCC-NR2013 submitted.pdf. [Accessed: 06 May 2014].

[12] J. Hopcroft, R. Motwani and J. Ullman, *Introduction to Automata Theory, Languages, and Computation*. Boston: Pearson Addison Wesley, 2007.

[13] Android. (2015). “Wi-Fi peer-to-peer.” [Online]. Available: http://developer.android.com/guide/topics/connectivity/wifip2p.html. [Accessed: 29 Nov. 2013].

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California